(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 49 292 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
H 04 L 12/22
H 04 N 7/16
G 07 C 9/00

(21) Aktenzeichen: 196 49 292.0
(22) Anmeldetag: 28. 11. 96
(43) Offenlegungstag: 4. 6. 98

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Schwenk, Jörg, Dr.rer.nat., 64846 Groß-Zimmern, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

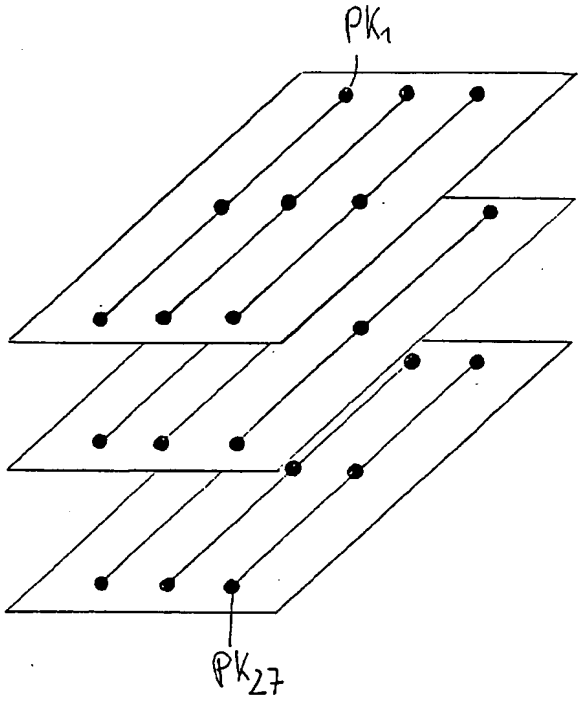
DE	43 26 590 C1
DE	38 27 172 C2
DE	34 32 653 C1
DE	195 11 298 A1
DE	195 11 298 A1
DE	43 35 835 A1
DE	33 25 858 A1
DE	31 24 150 A1
US	49 10 773
US	48 88 801
US	47 71 459
US	43 09 569
EP	05 06 435 A2
WO	95 09 500 A1

CHOKHANI,Santosh: Toward a National Public Key Infrastructure. In: IEEE Communications Magazine, Sep. 1994, S.70-74;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zum Sichern eines durch eine Schlüsselhierarchie geschützten Systems

(57) Die Erfindung betrifft ein Verfahren zum Sichern wenigstens eines durch eine vorbestimmte Hierarchie von kryptografischen Schlüsseln geschützten Systems, insbesondere eines Pay-TV-Systems, gegen unberechtigte Nutzer. In Schlüsselhierarchie-Systemen gibt es derzeit keine Möglichkeit, einen unzuverlässigen Kunden zu ermitteln, der einen vom Systembetreiber übermittelten Gruppenschlüssel kopiert und an beliebige Personen weiterveräußert hat. Die Erfindung schlägt als Lösung vor, daß wenigstens ein, einem unzuverlässigen Nutzer zugeordneter, individueller kryptografischer Schlüssel ermittelt wird, indem die Schnittmenge von wenigstens zwei vorbestimmten, zu verschiedenen Zeitpunkten gebildeten Teilmengen, die der gleichen Hierarchieebene angehören, gebildet wird.



Beschreibung

Die Erfindung betrifft ein Verfahren zum Sichern wenigstens eines durch eine vorbestimmte Hierarchie von kryptografischen Schlüsseln geschützten Systems, insbesondere eines Pay-TV-Systems, gegen unberechtigte Nutzer gemäß Anspruch 1.

Auf vielen Einsatzgebieten wird eine Schlüsselhierarchie verwendet, um aus den individuellen kryptografischen Schlüsseln der Kunden einen für eine große Anzahl von Kunden gemeinsamen Schlüssel abzuleiten. Ein typischer Anwendungsfall stellt ein Pay-TV-System dar. Mit Hilfe einer Schlüsselhierarchie ist es möglich, die Erlaubnis zum Empfang eines Pay-TV-Programms selektiv nur an ausgewählte Kunden zu verteilen. Eine mögliche Schlüsselhierarchie weist die Form einer Baumstruktur auf. In der untersten Hierarchieebene erhält jeder potentielle Kunde zunächst eine Chipkarte oder ein anderes Sicherheitsmodul, auf der ein individueller, eindeutig dem Kunden zugeordneter Schlüssel gespeichert ist. Der Pay-TV-Programmanbieter speichert alle diese individuellen kryptografischen Schlüssel in einer zentralen Speichereinrichtung. Stufenweise wird danach die Schlüsselhierarchie aufgebaut, indem in der zweiten Ebene zunächst die Schlüssel der untersten Ebene zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt werden. Jeder Teilmenge wird ein kryptografischer Gruppenschlüssel zugeordnet, der mit Hilfe der die kryptografischen Schlüssel der untersten Ebene, die die jeweilige Teilmenge bilden, übermittelt wird. Anschließend werden in der dritten Ebene die Teilmengen der zweiten Ebene zu mehreren Teilmengen zusammengefaßt, wobei jede Teilmenge der dritten Ebene größer ist als jede Teilmenge der zweiten Ebene. Jeder Teilmenge der dritten Ebene wird ein kryptografischer Gruppenschlüssel zugeordnet, der mit Hilfe der kryptografischen Gruppenschlüssel der zweiten Ebene, die die jeweilige Teilmenge bilden, übermittelt wird. Dieses Verfahren kann solange fortgesetzt werden, bis ein gemeinsamer Schlüssel für die Kunden, die zum Empfang des Pay-TV-Programms berechtigt sind, generiert ist. Auf ein solches, durch eine Schlüsselhierarchie geschütztes System sind verschiedene Angriffe denkbar, die alle davon ausgehen, daß ein unzuverlässiger Kunde den individuellen Schlüssel, einen oder mehrere Gruppenschlüssel oder den gemeinsamen Schlüssel, die auf seiner oder einer anderen Chipkarte gespeichert sind, kennt und diese unberechtigterweise an beliebige Dritte weitergibt. Man unterscheidet drei mögliche Angriffe auf ein solches System:

1. Der unzuverlässige Kunde kopiert den gemeinsamen Schlüssel und gibt diesen unberechtigterweise, z. B. auf einer Piratenchipkarte, an andere Personen weiter. Dieser Angriff kann dadurch abgewehrt werden, daß der Systembetreiber, der die kryptografischen Schlüssel generiert, den gemeinsamen Schlüssel in entsprechend kurz gewählten Zeitintervallen neu generiert.
2. Ein unzuverlässiger Kunde kopiert seinen individuellen kryptografischen Schlüssel und gibt diesen unberechtigterweise an andere Personen weiter. In diesem Fall kann der Kunde relativ einfach von der Nutzung des Systems ausgeschlossen werden, wenn der kopierte individuelle Schlüssel, z. B. auf einer Piratenkarte, erkannt wird. Denn zwischen dem individuellen kryptografischen Schlüssel und der dazugehörigen Person besteht ein eindeutiger Zusammenhang.
3. Ein unzuverlässiger Kunde kopiert einen Gruppenschlüssel und gibt diesen weiter. In diesem Fall ist es ohne weiteres nicht möglich, den unzuverlässigen Kunden eindeutig anhand des kopierten Gruppenschlüssels zu identifizieren. Der Systembetreiber muß entweder alle Kunden der durch den Gruppenschlüssel identifizierten Gruppe von der Benutzung des Systems ausschließen oder den Mißbrauch durch den kopierten Gruppenschlüssel tolerieren.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren bereitzustellen, mit dem ein durch eine Schlüsselhierarchie geschütztes System gegen unberechtigte Nutzer effektiver geschützt werden kann.

Dieses technische Problem löst die Erfindung mit den Verfahrensschritten des Anspruchs 1.

Jedem potentiellen Systemnutzer wird in der untersten Ebene der Schlüsselhierarchie ein individueller kryptografischer Schlüssel zugeordnet, der ihm beispielsweise durch eine Chipkarte oder ein anderes Sicherheitsmodul ausgehändigt werden kann. Die individuellen kryptografischen Schlüssel jedes Nutzers werden in einer dem System zugeordneten Speichereinrichtung abgespeichert. Zu vorbestimmten diskreten Zeitpunkten wird anschließend wenigstens eine höhere Hierarchieebene von kryptografischen Schlüsseln durch folgende Schritte gebildet: die kryptografischen Schlüssel der unmittelbar niedrigeren Hierarchieebene werden in beliebiger Weise zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt, wobei jeder Teilmenge ein kryptografischer Schlüssel zugeordnet wird, der mit Hilfe der die jeweilige Teilmenge bildenden kryptografischen Schlüssel übermittelt und anschließend in der Speichereinrichtung abgelegt wird. Danach wird wenigstens ein, einem verdächtigen Nutzer zugeordneter individueller kryptografischer Schlüssel ermittelt, indem die Schnittmenge von wenigstens zwei vorbestimmten, zu verschiedenen Zeitpunkten gebildeten Teilmengen, die der gleichen Hierarchieebene angehören, gebildet wird.

Vorteilhafte Weiterbildungen sind in den Unteransprüchen angegeben.

Statt zu vorbestimmten diskreten Zeitpunkten die höheren Hierarchieebenen neu zu bilden, können für unterschiedliche Systembetreiber gleichzeitig verschiedene Schlüsselhierarchien erzeugt werden. Jede Schlüsselhierarchie weist wenigstens eine höhere Hierarchieebene von kryptografischen Schlüsseln auf. Eine höhere Hierarchieebene wird dadurch gebildet, daß die kryptografischen Schlüssel der unmittelbar niedrigeren Hierarchieebene in beliebiger Weise zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt werden, wobei jeder Teilmenge ein kryptografischer Schlüssel zugeordnet wird, der aus den, die jeweilige Teilmenge bildenden kryptografischen Schlüssel generiert und anschließend in der Speichereinrichtung abgelegt wird. Danach wird wenigstens ein, einem verdächtigen Nutzer zugeordneter individueller kryptografischer Schlüssel ermittelt, indem die Schnittmenge von wenigstens zwei vorbestimmten Teilmengen, die der gleichen Hierarchieebene verschiedener Schlüsselhierarchien angehören, gebildet wird.

Man kann zur Realisierung dieses Verfahrens sukzessive immer größere Teilmengen entsprechend der Anzahl von Hierarchieebenen bilden. Ein mögliches Beispiel hierfür wäre eine Schlüsselhierarchie in Baumstruktur. Eine besonders effiziente Lösung ergibt sich jedoch, wenn man geometrische Strukturen verwendet, um die kryptografischen Schlüssel zu Teilmengen vorbestimmter Größe zusammenzufassen. Geometrische Strukturen bieten den Vorteil, daß die Eigenschaften der Schnittmengenbildung verschiedener Teilmengen sehr gut beschrieben werden können.

Vorzugsweise kann eine für mehrere Kunden erzeugte Schlüsselhierarchie mit Hilfe eines endlichen affinen Raums AG(d,q) der Dimension d über dem Körper GF(q) realisiert

werden (siehe A. Beutelspacher, Einführung in die endliche Geometrie I & II, BI Wissenschaftsverlag 1982, und A. Beutelspacher und U. Rosenbaum, Projektive Geometrie, Vieweg Verlag, 1992).

Die Schnittmengenbildung wird noch einfacher, wenn die geometrische Struktur ein endlicher projektiver Raum PG(d,q) der Dimension d über dem Körper GF(g) ist.

Die Erfindung wird nachfolgend anhand mehrerer Ausführungsbeispiel in Verbindung mit den beiliegenden Zeichnungen näher erläutert. Es zeigen:

Fig. 1 eine Schlüsselhierarchie für vier berechtigte Teilnehmer in Baumstruktur, die zu einem ersten Zeitpunkt gebildet worden ist,

Fig. 2 eine Schlüsselhierarchie nach **Fig.** 1, die jedoch zu einem zweiten Zeitpunkt generiert worden ist,

Fig. 3 eine Schlüsselhierarchie für 27 Teilnehmer des affinen Raums AG(**3**,**3**), die zu einem ersten Zeitpunkt gebildet worden ist,

Fig. 4 eine Schlüsselhierarchie nach **Fig.** 3, die zu einem zweiten Zeitpunkt erzeugt worden ist, und

Fig. 5 zwei verschiedene, zur gleichen Zeit existierende Schlüsselhierarchien.

In **Fig.** 1 ist eine Schlüsselhierarchie in Baumstruktur beispielsweise für ein Pay-TV-System dargestellt, das beispielsweise fünf Kunden umfaßt. Jeder Kunde i erhält von einem Systembetreiber oder Pay-TV-Programmanbieter einen individuellen kryptografischen Schlüssel PK_i, der in der untersten Hierarchieebene angeordnet wird. Die unterste Hierarchieebene enthält somit fünf individuelle kryptografische Schlüssel PK_1–PK_5. Der Anbieter speichert diese Schlüssel in einer zentralen Speichereinrichtung. Mit Hilfe der verwendeten Baumstruktur ist es nunmehr möglich, ausgewählten Kunden die Erlaubnis zum Empfang eines Pay-TV-Programms einzuräumen. Beispielsweise sollen nur die Kunden 1, 2, 3, und 4 zum Empfang des TV-Programms authorisiert werden, der Kunde 5 dagegen nicht. Um diese Berechtigungszuweisung zu erreichen, werden die Kunden 1 bis 4 in der nächst höheren Hierarchieebene – das ist die zweite Ebene – vorteilhafterweise zu zwei Teilmengen mit jeweils zwei Kunden zusammengefaßt. In der Praxis geschieht dies dadurch, daß in einer zentralen Stelle zunächst für die beiden Teilmengen jeweils ein Gruppenschlüssel GK_1 bzw. GK_2 generiert wird. Der Gruppenschlüssel GK_1 wird mit Hilfe der beiden individuellen kryptografischen Schlüssel PK_1 und PK_2 der Kunden 1 bzw. 2 übertragen, wohingegen der Gruppenschlüssel GK_2 mit Hilfe der beiden individuellen kryptografischen Schlüsseln PK_3 und PK_4 der Kunden 3 bzw. 4 übertragen wird. Die Kunden 1 und 2 können mittels ihres individuellen kryptografischen Schlüssel PK_1 bzw. PK_2 den Gruppenschlüssel GK_1 berechnen, wohingegen die Kunden 3 und 4 mittels ihrer individuellen kryptografischen Schlüssel PK_3 bzw. PK_4 den Gruppenschlüssel GK_2 berechnen können. Der Kunde 5 hingegen kann keinen der beiden Gruppenschlüssel entschlüsseln. In der höchsten Hierarchieebene – das ist hier die dritte Ebene – wird danach eine Gesamtmenge gebildet, die die beiden Teilmengen der unmittelbar darunterliegenden Ebene **2** und damit die vier berechtigten Kunden enthält. In der zentralen Stelle wird dazu ein gemeinsamer Schlüssel SK mit Hilfe der beiden Gruppenschlüssel GK_1 und GK_2 der zweiten Ebene übertragen. Da das vom Anbieter ausgestrahlte Pay-TV-Programm mit dem gemeinsamen Schlüssel SK verschlüsselt ist, können die Kunden 1 bis 4 das Programm entschlüsseln und empfangen, der Kunde 5 hingegen nicht. Die in **Fig.** 1 dargestellte Schlüsselhierarchie umfaßt beispielhaft drei Hierarchieebenen.

Die Erfindung beschäftigt sich nunmehr mit dem Problem, einen unzuverlässigen Kunden ausfindig zu machen, der einen Gruppenschlüssel GK_1 oder GK_2 kopiert und unberechtigterweise an Dritte weitervertreiben hat. Der unzuverlässige Kunde kann die "gestohlenen" Gruppenschlüssel in Form von Piraten-Chipkarten veräußern oder auch unter einer e-Mail-Adresse anbieten. Es sei angenommen, daß es sich bei dem Kunden 4 um den unzuverlässigen Kunden, nachfolgend auch Pirat genannt, handelt, der den Gruppenschlüssel GK_2, der von der zentralen Stelle zuvor rundgesendet worden ist, kopiert und nun an beliebige Dritte weiterveräußert hat. Wenn der Systembetreiber in den Besitz des kopierten Gruppenschlüssels GK_2 kommt, kann er den Piraten nicht eindeutig ermitteln, da der Gruppenschlüssel GK_2 den beiden Kunden 3 und 4 zugeordnet ist. Es ist nun Ziel der Erfindung, den unzuverlässigen Kunden 4 aus der Gruppe von Kunden herauszufinden, die durch den Gruppenschlüssel GK_2 identifiziert sind. Dazu wird die verdächtige Gruppe mit ihrem zugeordneten kryptografischen Schlüssel GK_2 in der zentralen Stelle abgespeichert. Zu einem vorbestimmten Zeitpunkt generiert die zentrale Stelle eine neue Schlüsselhierarchie, die in **Fig.** 2 dargestellt ist, gebildet. Dazu werden willkürlich zwei neue Teilmengen gebildet, die beispielsweise die Kunden 1, 3 bzw. 2 und 4 umfassen. Die Neubildung der Teilmengen wird in der zentralen Stelle verwirklicht, indem für jede Teilmenge ein neuer Gruppenschlüssel GK_1' bzw. GK_2' generiert wird. Darüber hinaus wird auch ein neuer gemeinsamer Schlüssel SK' erzeugt. Die Vorgehensweise zur Erzeugung von Gruppenschlüssel und eines gemeinsamen Schlüssels wurde bereits oben ausführlich erläutert worden ist. Die neu generierten kryptografischen Schlüssel werden wiederum zu den einzelnen Kunden ausgesendet und in der zentralen Stelle abgespeichert. Der Pirat, in unserem Fall der Kunde 4, ist nunmehr gezwungen, den neuen Gruppenschlüssel GK_2' zu kopieren und an beliebige Personen zu verteilen. Sobald die zentrale Stelle im Besitz des kopierten Gruppenschlüssels GK_2' ist, wird dieser in der zentralen Speichereinrichtung abgespeichert. Anschließend wird die Schnittmenge aus der Teilmenge, der der kryptografische Gruppenschlüssel GK_2 zugeordnet ist, und der Teilmenge, der der kryptografische Gruppenschlüssel GK_2' zugeordnet ist, ermittelt. Da die zum ersten Zeitpunkt (s. **Fig.** 1) gebildete Teilmenge die Kunden 3 und 4 und die zum zweiten Zeitpunkt (s. **Fig.** 2) gebildete Teilmenge die Kunden 2 und 4 enthält, ergibt sich als Schnittmengen der Kunde 4. Die zentrale Stelle kennt nun den unzuverlässigen Kunden und kann ihn von der Nutzung des Systems ausschließen, indem beispielsweise sein individueller kryptografischer Schlüssel PK_4 gesperrt wird. Obwohl die in **Fig.** 1 und 2 gezeigten Schlüsselhierarchien nur vier Kunden erfassen, können Schlüsselhierarchien beliebiger Größe verwendet werden. Damit erhöht sich selbstverständlich auch der Aufwand, einen unzuverlässigen Kunden zu finden, da die Anzahl der Gruppen größer ist. In **Fig.** 3 und 4 sind zwei zu unterschiedlichen Zeitpunkten gebildete Hierarchien von Teilmengen beschrieben, die mit Hilfe des endlichen affinen Raums AG(**3**,**3**) der Dimension 3 über den Körper GF(**3**) realisiert werden können. Der in **Fig.** 3 und 4 dargestellte affine Raum besteht aus 27 Punkten, die den potentiellen Pay-TV-Kunden entsprechen. Es ist vorteilhaft, die Hierarchie von Teilmengen mit Hilfe des endlichen affinen Raums zu realisieren, da damit die Eigenschaften der Schnittmengenbildung verschiedener Teilmengen sehr genau beschrieben werden kann. **Fig.** 3 zeigt die zu einem ersten Zeitpunkt gebildete Hierarchie. Jedem Kunden wird wieder ein individueller kryptografischer Schlüssel PK_1 bis PK_{27} bereitgestellt. Man kann sich nun vorstellen, daß jedem Punkt des affinen Raums ein kryptografischer Schlüssel des jeweiligen Kunden zugeordnet ist. Die 27 Punkte können sukzessive zu Teilmengen von drei bzw. neun Punkten

zusammengefaßt werden, indem man zunächst neun parallele Geraden auswählt und danach drei parallele Ebenen, die mit den Geraden verträglich sein müssen. Mit anderen Worten müssen die Geraden jeweils vollständig in einer der drei Ebenen enthalten sein. Übertragt man diese Struktur auf eine Schlüsselhierarchie, liegen die einzelnen Punkte in der untersten Ebene, die Geraden in der zweiten Ebene, die drei Ebenen des affinen Raumes in der dritten Ebene, wobei die höchste Hierarchieebene den gesamten, die einzelnen Punkte, die neun Geraden und drei Ebenen umfassenden Raum enthält. In der zentralen Stelle werden nach dem bereits ausführlich beschriebenen Verfahren für jede Gerade, für jede Ebene des affinen Raums Gruppenschlüssel und für den Raum selbst ein gemeinsamer, alle Kunden umfassender Schlüssel generiert. Der Vorteil der geometrischen Strukturen und insbesondere von affinen Räumen besteht nun darin, daß man genau angeben kann, wieviele Teilmengen (Geraden oder Ebenen) man kennen muß, um einen bestimmten Punkt zu ermitteln. So schneiden sich beispielsweise zwei nichtparallele Ebenen eines affinen Raums genau in einer Geraden, und drei paarweise nichtparallele Ebenen in genau einem Punkt. Um beispielsweise den individuellen Schlüssel eines Piraten zu ermitteln, der den Gruppenschlüssel einer Ebene (das entspricht einer Gruppe von neun Personen) des affinen kopiert und weiterveräußert hat, genügt es, den affinen Raum zu drei diskreten Zeitpunkten derart in neue Ebenen aufzuteilen, daß die Ebenen nicht parallel zueinander verlaufen. Mit anderen Worten möchte man einen unzuverlässigen Kunden aus den 27 Kunden ermitteln, müssen neben den in **Fig.** 3 und 4 zu unterschiedlichen Zeitpunkten gebildeten Hierarchien noch eine dritte, zu einem dritten Zeitpunkt gebildete Hierarchie erzeugt werden. Werden die drei paarweise nicht parallelen Ebenen, denen jeweils ein bestimmter Gruppenschlüssel zugeordnet ist, miteinander geschnitten, so erhält man einen gemeinsamen Schnittpunkt, der dem unzuverlässigen Kunden entspricht. Die zentrale Stelle muß nur noch veranlassen, daß der zu dem unzuverlässigen Kunden gehörende individuelle kryptografische Schlüssel gesperrt wird.

Noch einfacher wird das Verfahren zur Ermittlung eines unzuverlässigen Kunden durch Schnittmengenbildung, wenn endliche projektive Räume anstelle von endlichen affinen Räumen verwendet werden, da man hier nicht zwischen parallelen und nichtparallelen Strukturen unterscheiden muß. Die oben beschriebenen Verfahren können auch angewendet werden, wenn ein unzuverlässiger Kunde mehrere individuelle Schlüssel kopiert und diese abwechselnd einsetzt. In diesem Fall müssen aber deutlich mehr Hierarchien zu unterschiedlichen Zeitpunkten gebildet werden. Kennt z. B. ein Pirat zwei von neun individuellen kryptografischen Schlüsseln, so muß die affine Ebene insgesamt drei Mal neu in parallele Geraden aufgeteilt werden, um eine fälschliche Identifizierung eines berechtigten Teilnehmers auszuschließen und einen der beiden Schlüssel zu identifizieren.

Anstatt zur Ermittlung des individuellen Schlüssels eines Piraten mehrere Schlüsselhierarchien zu vorbestimmten Zeitpunkten zu bilden müssen, ist es auch vorstellbar, daß verschiedene Schlüsselhierarchien zur gleichen Zeit existieren. In **Fig.** 5 sind zwei verschiedene Schlüsselhierarchien dargestellt. Mehrere gleichzeitig existierende Schlüsselhierarchien sind sinnvoll, wenn sich mehrere Diensteanbieter eine Kundenchipkarte teilen. Es sei angenommen, daß der Kunde 2 den die beiden Kunden 1 und 2 enthaltenden Gruppenschlüssel 10 des einen Dienstcanbieters und den die Kunden 2, 3 und 4 enthaltenden Gruppenschlüssel 20 des anderen Diensteanbieters kopiert und weiterveräußert habe. In diesem Fall kann man den unzuverlässigen Kunden wiederum durch Bildung der Schnittmengen der zugehörigen Gruppen 10 und 20 bestimmen. Wie unteranderem aus **Fig.** 5 zu erkennen ist, müssen die Teilmengen derselben Hierarchieebene nicht notwendigerweise die gleiche Größe aufweisen.

Patentansprüche

1. Verfahren zum Sichern wenigstens eines durch eine vorbestimmte Hierarchie von kryptografischen Schlüsseln geschützten Systems, insbesondere eines Pay-TV-Systems, gegen unberechtigte Nutzer mit folgenden Verfahrensschritte:

   a) jedem Systemnutzer wird in der untersten Hierarchieebene ein individueller kryptografischer Schlüssel zugeordnet;

   b) die individuellen, kryptografischen Schlüssel werden in einer dem System zugeordneten Speichereinrichtung abgespeichert;

   c) zu vorbestimmten diskreten Zeitpunkten wird wenigstens eine höhere Hierarchieebene von kryptografischen Schlüsseln durch folgende Schritte gebildet:

      – die kryptografischen Schlüssel der unmittelbar niedrigeren Hierarchieebene werden in beliebiger Weise zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt, wobei jeder Teilmenge ein kryptografischer Schlüssel zugeordnet wird, der mit Hilfe der die jeweilige Teilmenge bildenden kryptografischen Schlüssel übertragen und anschließend in der Speichereinrichtung abgelegt wird;

   d) Ermitteln wenigstens eines, einem Nutzer zugeordneten individuellen kryptografischen Schlüssels, indem die mengentheoretische Schnittmenge von wenigstens zwei vorbestimmten, zu verschiedenen Zeitpunkten gebildeten Teilmengen, die der gleichen Hierarchieebene angehören, gebildet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Schritte c) und d) ersetzt werden durch die Schritte:

   c') für jedes System werden gleichzeitig wenigstens zwei höhere Hierarchieebene von kryptografischen Schlüsseln durch folgende Schritte gebildet:

   – die kryptografischen Schlüssel der unmittelbar niedrigeren Hierarchieebene werden in beliebiger Weise zu mehreren Teilmengen vorbestimmter Größe zusammengefaßt, wobei jeder Teilmenge ein kryptografischer Schlüssel zugeordnet wird, der mit Hilfe der die jeweilige Teilmenge bildenden kryptografischen Schlüssel übertragen und anschließend in der Speichereinrichtung abgelegt wird;

   d') Ermitteln wenigstens eines, einem Nutzer zugeordneten individuellen kryptografischen Schlüssels, indem die mengentheoretische Schnittmenge von wenigstens zwei vorbestimmten Teilmengen, die der gleichen Hierarchieebene verschiedener Schlüsselhierarchien angehören, gebildet wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Zusammenfassen der kryptografischen Schlüssel zu Teilmengen vorbestimmter Größe durch endliche geometrische Strukturen festgelegt wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die geometrische Struktur ein endlicher affiner Raum AG(d,q) der Dimension d über dem Körper GF(q) ist.

5. Verfahren zur Ermittlung eines kryptographischen Schlüssels nach Anspruch 3, dadurch gekennzeichnet, daß die geometrische Struktur ein endlicher projektiver Raum PG(d,g) der Dimension d über dem Körper GF(q) ist.

Hierzu 4 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 196 49 292 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 4. Juni 1998

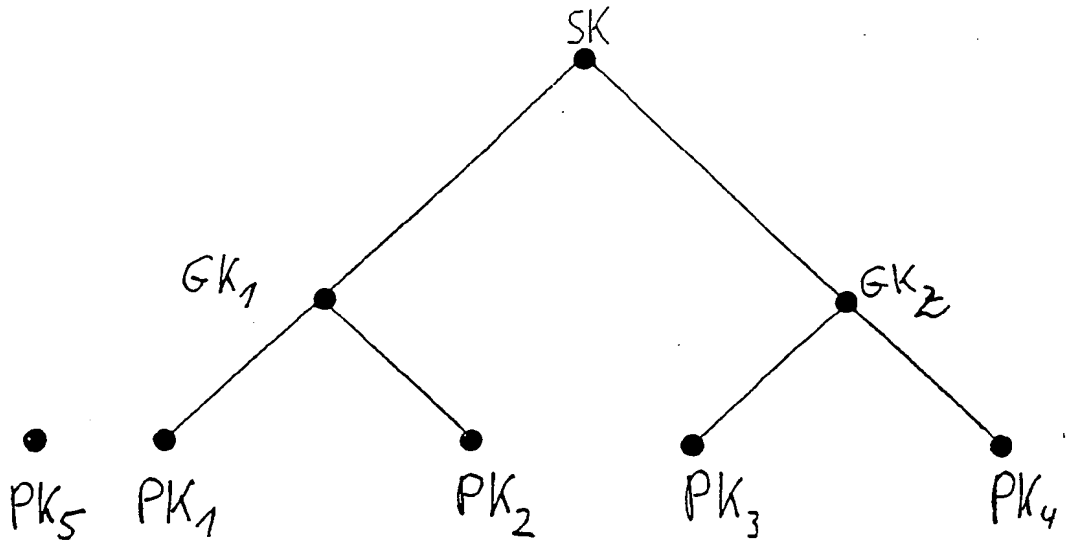


Fig. 1

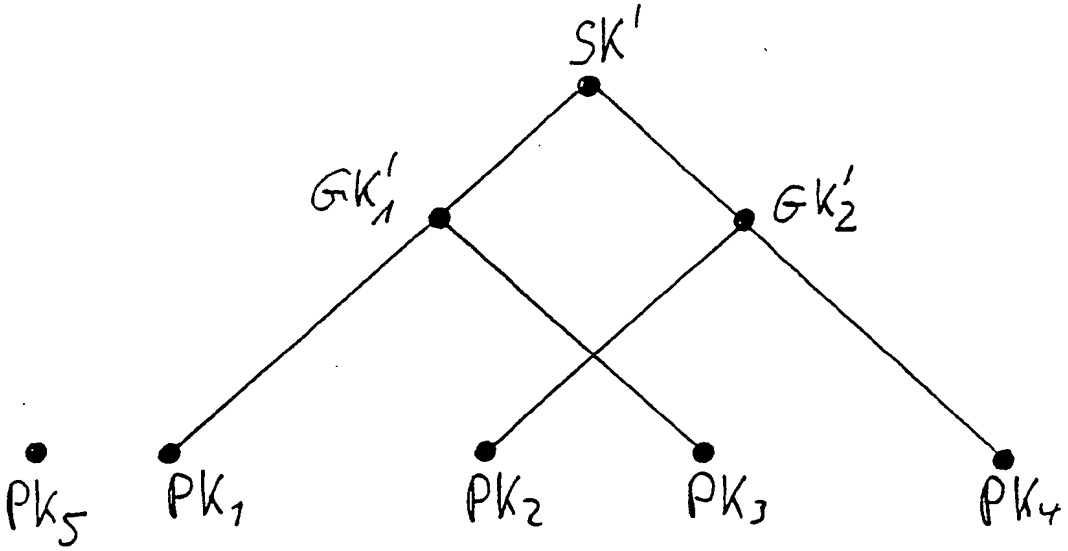


Fig. 2

Nummer: DE 196 49 292 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 4. Juni 1998

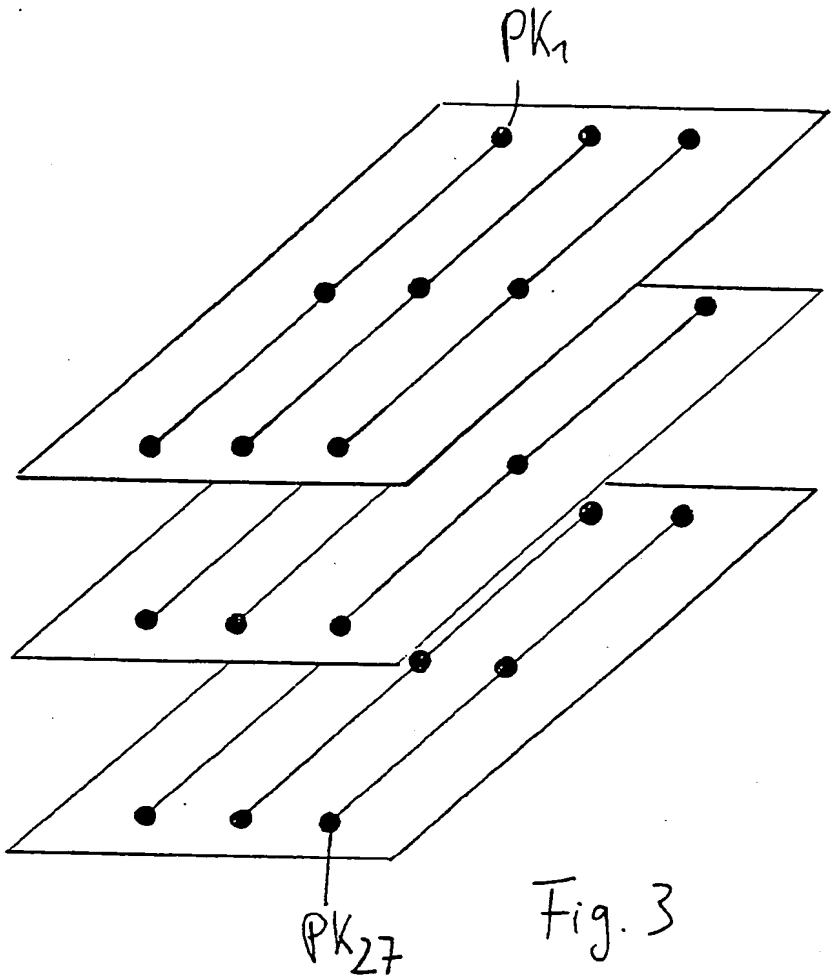


Fig. 3

Nummer: DE 196 49 292 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 4. Juni 1998

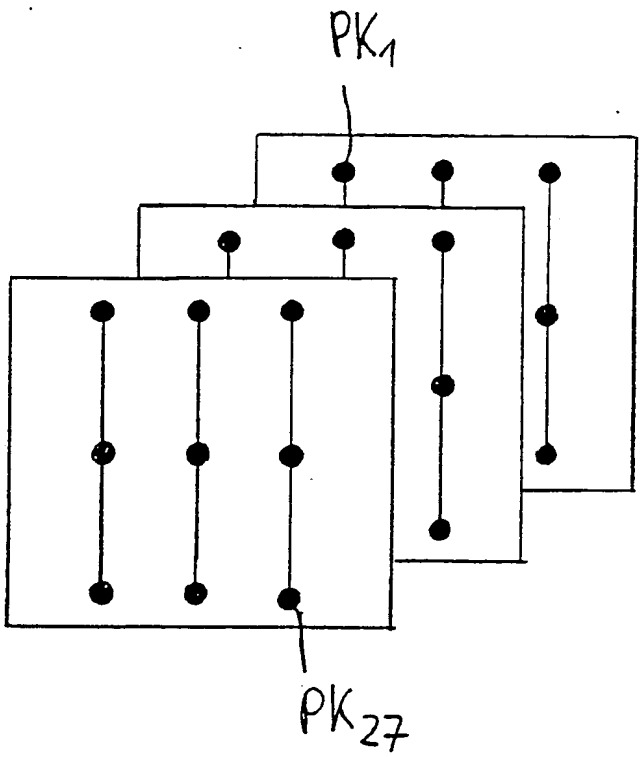


Fig. 4

Nummer: DE 196 49 292 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 4. Juni 1998

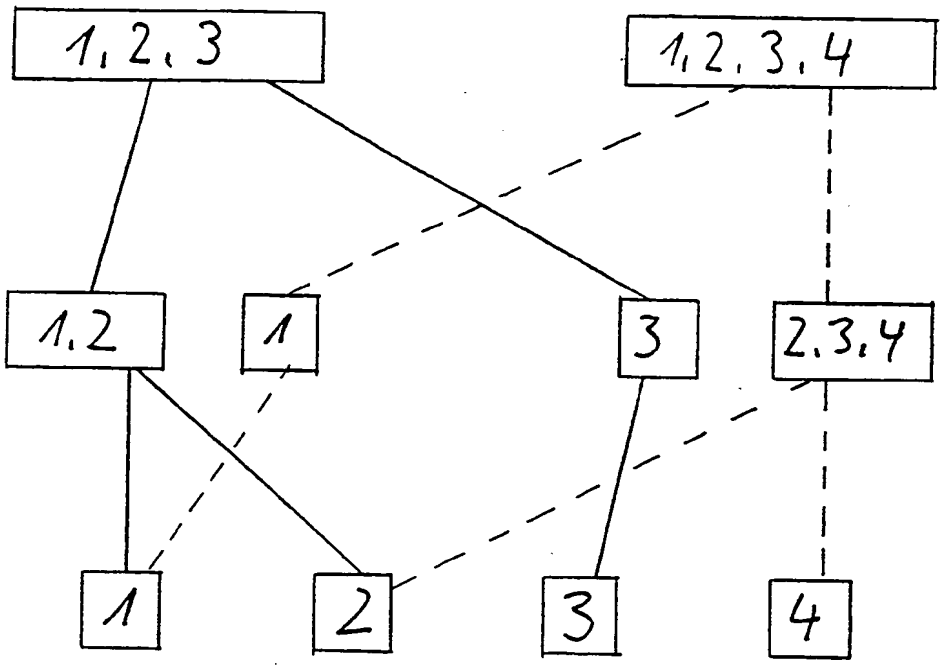


Fig. 5